UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/690,017	10/21/2003	James P. Goddard	END920030107US1	4833

26502 7590 11/15/2006

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
HOANG, DANIEL L	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/690,017	GODDARD, JAMES P.	
	Examiner	Art Unit	
	Daniel L. Hoang	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5/17/2003, 10/06/2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 May 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/06/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldfeder et al., US PGP 20040230835, hereinafter Gold, further in view of Turkboylari (US PGP No. 20030140238), hereinafter Turbo.

As per claim 1 and 22-24, Gold teaches:

A method for evaluating a security risk of an application,

> *[see paragraph 6] "A system and method for accumulating security assessment information about a program."*
>
> *[see paragraph 35] "The Trust Manager begins evaluating the security risks of the application by invoking a series of Trust Evaluators that each evaluate a specific area of security risk. For instance a virus evaluator may be configured to examine each component of an application for the possibility that the application contains a virus. A privacy evaluator may evaluate the permissions requested by the application to determine what level of threat to privacy the application presents. Many other Trust Evaluators may also be used, as will be apparent to those skilled in the art.*

said method comprising the steps of:

determining mitigation controls for the security risk of said application; and assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the determination in evaluating said security risk.

> *[see paragraph 36] "Loop 508 is performed for each Trust Evaluator in the system. The Loop 508 begins at block 509, where the current Trust Evaluator examines the information in the ADO and/or the components of the application to assess the security risk. The information in the ADO may be compared against a set of rules or other criteria to build a score that quantifies the security risk of the application. In one example, a score may be a value from zero (maximum risk) to one (minimum risk).*

Gold teaches the use of "trust evaluators" that are used to assess security risks. Gold cites, as examples, possible security risks including viruses and privacy threats. Gold does not explicitly cite that his system assesses security risks such as unauthorized access, loss of data, third-party attack vulnerabilities, and different customers sharing the application. Such security risks are well known. Below are security risks as taught by Turbo (US PGP No. 20030140238).

determining whether unauthorized access or loss of said data would cause substantial damage;

> *[see paragraph 4] "Especially in recent years, the security of computer systems has become an important issue in the computer industry. Operators of computer systems are rightfully concerned about the security of electronically stored information from unauthorized access, especially regarding sensitive and valuable business information."*
>
> *[see paragraph 4] "The disruption of computer networks, as well as the destruction of data or loss of secrecy to such data, can cause significant damage to modern business and government entities, not to mention to individual persons. In addition, the computer systems themselves can be compromised by electronic vandalism, so as to be temporarily or permanently disabled."*

determining whether said application is vulnerable to attack by a third party and whether the application is shared by different customers;

> *[see paragraph 4] "Also as is well known in the art and by the general public, malicious attacks of computer systems by way of computer viruses, and also by way of unauthorized access to computer networks, are also of significant concern."*

It would have been obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to include an assessment of the above well-known security risks in the security assessment system taught by Gold in order to "protect a user from multiple disparate security risks presented by a particular software program when it is being downloaded, installed, or executed."

As per claim 2, Turbo teaches:

A method as set forth in claim 1 further comprising the step of determining whether said application is vulnerable to allow a third party unauthorized write access to data maintained by or accessed by said application.

> *[see rejection of claim 1 wherein "Operators of computer systems are rightfully concerned about the security of electronically stored information from unauthorized access, especially regarding sensitive and valuable business information."]*

As per claim 3,

A method as set forth in claim 1 further comprising the step of determining whether said application is subject to industry controls.

Industry controls and regulations are well known in the art. Industry controls are especially well known in government settings where users are subject to higher controls because information within such a setting may require that higher security protocols be in place. It would be obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to include the above security assessment in order to increase the level of security of the system where such controls exist.

As per claim 4,

A method as set forth in claim 1 further comprising the step of determining whether said data is personal in nature.

Turbo teaches above the concerns pertaining to unauthorized access of data. It is well known that computer applications can have access to personal information such as personal addresses or social security numbers. It would have been obvious to one of ordinary skill in the art to which the subject matter pertains to include an assessment of whether data is personal in nature in order to prevent unauthorized access to such data.

As per claim 5,

A method as set forth in claim 1 further comprising the step of determining whether there is a known exploit for said application.

CERT Advisories are well known in the art. It would be obvious to a person of ordinary skill in the art at the time of the invention to which the subject matter pertains to utilize CERT Advisories in order to analyze and reduce possible cyber threats and vulnerabilities.

As per claim 6,

A method as set forth in claim 1 further comprising the step of determining whether an exploit for said application could be created.

It would be obvious to one of ordinary skill in the art in the art at the time of the invention to which the subject matter pertains to determine whether an exploit for the application could be created in order to prevent such exploit from occurring.

As per claim 7,

A method as set forth in claim 1 further comprising the step of determining whether said application is vulnerable to allow a third party unauthorized read access to said data.

[see rejection of claim 2]

As per claim 8,

A method as set forth in claim 1 further comprising the steps of: determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and assigning a numerical value or weight corresponding to a significance of said security risk to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs.

It would have been obvious to one of ordinary skill in the art at the time of the invention to which the subject matter pertains to include within the system taught by Gold, a step of determining vulnerabilities of a system that can be caused by outsiders of the system that are not authenticated to use the program. This would be advantageous because security risks are present both inside and outside of an organization.

As per claim 9,

A method as set forth in claim 1 further comprising the step of determining whether data maintained by or accessed by said application is confidential.

> [see rejection of claim 1, wherein "*The disruption of computer networks, as well as the destruction of data or loss of secrecy to such data, can cause significant damage to modern business and government entities.*"]

It is well known that government entities can have access to confidential information thus it would be obvious to determine whether data being maintained or accessed by the application is confidential.

As per claim 10,

A method as set forth in claim 1 further comprising the step of determining whether a customer has direct use of said application.

> *[see Goldstone, paragraph 2] "Computer users today have access to a multitude of different applications and utilities. The typical computer user may install dozens of computer programs on a computer over the course of a year. Most times, computer users knowingly install programs on their computers."*

It is clear that the user has direct use of the application being installed.

As per claim 11,

A method as set forth in claim 1 further comprising the step of determining whether said application is subject to industrial controls for security.

> [see rejection of claim 5]

As per claim 12,

A method as set forth in claim 1 wherein said mitigation controls comprise an intrusion detection system.

Intrusion detection systems are well known in the art. Intrusion detection systems detect unwanted manipulations to computer systems. Turbo teaches above that unwanted access to data is undesirable. It would be obvious to one of ordinary skill in the art to modify the Gold reference to include an intrusion detection system as a mitigation control in order to prevent unwanted manipulation of the application because the application can have access to sensitive data.

[also see rejection of claim 1, "virus evaluator"]

As per claim 13,

A method as set forth in claim 1 wherein said mitigation controls comprise vulnerability scanning.

Vulnerability scanners are well known in the art. A vulnerability scanner is a computer program designed to search an application, computer or network for weaknesses. It would be obvious to one of ordinary skill in the art at the time of the invention to which the subject matter pertains to modify the Gold reference to include a vulnerability scanner to find holes in the system and plug them before they are exploited.

As per claim 14,

A method as set forth in claim 1 wherein said mitigation controls comprise health checking.

[see Gold, paragraph 24] "The Trust Manager 210 constructs a Trust Object 261 that describes the level of permissions with which the application will be loaded, if at all. The Trust Object 261 may include data that defines a permission grant set 262 for the application on a component-by-component basis.

As per claim 15,

A method as set forth in claim 1 wherein said mitigation controls comprise a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems.

[see Turbo, paragraph 37] "the secure bootloader is a bootloader with the additional functionality of authenticating program code as required, and then loading that code if authentication is successful."

As per claim 16,

A method as set forth in claim 1 further comprising the step of considering an importance of a customer of said application in evaluating the security risk of said application.

It would be obvious at the time of the invention to one of ordinary skill in the art to which the subject matter pertains to modify the Gold reference to consider the importance of a customer when

evaluating the security risk of an application. For example, certain users who attempt to use the application may be identified as known offenders based on previously collected data such as logging of IP addresses. Therefore, taking into account such information about said users will help in making the system more secure from known attackers.

As per claim 17,

A method as set forth in claim 1 further comprising the step of determining whether said application is vulnerable to allow a third party unauthorized administration authority.

[see rejection of claim 1 wherein unauthorized access is undesirable]

It would be obvious to screen for the above vulnerability because unauthorized administration authority could lead to unauthorized access to sensitive data.

As per claim 18,

A method as set forth in claim 1 further comprising the step of combining said numerical values or weights to evaluate said security risk.

[see rejection of claim 1, "score"]

As per claim 19,

A method as set forth in claim 1 further comprising the step of comparing said security risk to a cost savings provided by said application, and determining whether to certify said application for use based in part on said comparison.

It would be obvious to one of ordinary skill in the art at the time of the invention to which the subject matter pertains to compare the cost effect of allowing or disallowing the application. If allowing the application to be used is more costly then blocking use of the application then it would be more cost advantageous to block the application. Depending on the organization implementing the system, cost could be a mitigating factor in determining whether or not to certify the application.

As per claim 20,

A method as set forth in claim 1 further comprising the step of comparing said security risk to a revenue provided by said application, and determining whether to certify said application for use based in part on said comparison.

[see rejection of claim 19, wherein costs clearly have an effect on revenue.]

Conclusion

The following patents, pre-grant publications and NPL are cited to further show the state of the art with respect risk assessment.

US PGP No. 20050080720, to Betz, which is cited to show deriving security and privacy solutions to mitigate risk.

US PGP No. 20050065941, to DeAngelis, which is cited to show a system for optimizing business processes, complying with regulations and identifying threat and vulnerability risks for an enterprise.

US PGP No. 20060117388, to Nelson, which is cited to show a system for modeling information security risk.

US PGP No. 20030065929, to Milliken, which is cited to show a CERT Advisories.

IBM TDB No. NNRD453135, "Business Method of Using Host Based Health Checking and Vulnerability Mitigation"

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel L. Hoang
11/09/06

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/09/06